Artificial Intelligence Use in Project Management [1]

Projects, Project Managers, and Organizations Functioning in an AI Information Age

AI and Cybersecurity [2]

By Ivano di Filippo, Dr. Josh Ramirez,
Darrell Mesa, Claudia Alcelay and Rebecca Winston

Italy, Spain & USA

Introduction

First, one should set the parameters of what one means by cybersecurity. Cybersecurity is any tool, set of tools, processes, procedures, or practices that enable a person, organization, or nation to prevent, mitigate or alert one to a potential or active cyberattack. A cyberattack is a deliberate, illegal attempt to compromise the integrity, confidentiality, or availability of digital systems or information. When speaking of cybersecurity and artificial intelligence (AI), the same definitions hold true.

In this paper, the issue of cybersecurity and the potential impacts will be discussed, including means of cyberattacks, impacts, and steps that can be take through robust cybersecurity with the AI tools and systems in mind. One caveat to this overview is that the field is literally changing daily and the tools to combat cybersecurity in an AI system need to evolve and be developed strategically. Further, organizations, individuals, and nations need to understand the risks and determine whether they can afford to defend their systems and data and if not, what the cost of not investing in cybersecurity might mean. As noted by George Westerman, senior lecturer at the MIT Sloan School of Management, stated for a Sloan Management Review, “As [much as] we can do great stuff with these new tools, the hackers can also get a lot smarter — and much tougher to detect, . . .”. (https://sloanreview.mit.edu/article/video-8-ai-security-issues-leaders-should-watch/)

[1] *Editor’s note: This article is an introduction to a series of articles by the authors on the use of artificial intelligence (AI) in the project management field. While the authors recognize the rapidly growing attention on the potential power and impact of AI on project management, they also want to point out the risks of assuming AI and human intelligence are or can be equated. The authors have previously researched and published on topics related to neuro-behavioral issues and cognitive intelligence in project management.*

[2] How to cite this work: di Filippo, I., Ramirez, J., Mesa, D., Alcelay, C., Winston, R. (2024). AI and Cybersecurity; Projects, Project Managers, and Organizations Functioning in an AI Information Age; Artificial Intelligence Use in Project Management, series article 5, *PM World Journal*, Volume XIII, Issue X, October/November.

The paper does not deal with insider attacks, algorithms, and prompts, which can make the job of guarding against a cyberattack and maintaining cybersecurity that much harder.

This topic would be much easier if one could point to applicable industry standards, but to date there are none. The topic would also be easier if there were legislative regulations and rules governing AI and cybersecurity, but there are not. The regulations that currently exist under which some individuals and organizations have filed lawsuits from copyright to cyberattacks do not speak directly to the tools, models, or systems. Some governmental and quasi-governmental organizations have attempted to regulate the area in some respects, but to date none of these regulations have provided protection from cyberattacks. In other words, technology is way ahead of our ability to maintain privacy, proprietary information, and AI and other software tools safe from those individuals using cybersecurity to attack.

Cybersecurity and the AI tool and system

The risks faced when using an AI tool or system are both similar risks faced when doing searches on the internet or using cloud storage systems, but some of the risks are harder to prevent or mitigate in an AI environment and others are new to the tool. Having stated the risks can be similar, the overarching issue of trained, educated, and cybersecurity savvy personnel continues to be an issue across organizations. A survey done in November of 2023 found, “Only 17% of technologists are completely confident in their cybersecurity skills. And even less (12%) are completely confident in their AI/ML [artificial intelligence/machine learning] skills.” (Statista Research Services, Most Commonly Exploited Applications Worldwide from November 2021 to October 2022, statista.com)Part of the issue is the lack of hands-on training and education and the tremendous speed of evolution in the technology as well as learning on behalf of those creating the risk.

Some of the risks that exist are:

a. Deep fakes
b. Administrative “back doors” in the AI software architecture
c. Use of AI to create cyberattacks
d. Use of the organization’s own AI tool and system to launch attacks
e. Overwhelming array of cyberattacks
f. Cost of cyberattacks
g. Loss of proprietary information, and personnel and customer private information

Deep fakes rely on inadequate defenses to detect that the material is not from a trusted source. They also rely on human beings and their biases to comply with social norms and comply with social pressures. Once the attacker has been granted access to the

organization's system, the attacker can access many if not all the organization's environments depending on what information is targeted. The attacker is now in a position of learning and the learning has become easier with AI, especially since many of the attacks are now using AI to create and implement the numerous gates that the attacker must overcome, such as gaining the necessary access privileges to the various organizational environments, determining what tools or ransomware are needed, determining how to communicate with the command and control protocols (C2), and exfiltrate data and block recognition at each juncture to avoid not just detection but being caught.

The use of AI to implement these attacks is becoming more common. As with any use of AI the tool will "learn" as it is used, which benefits the attacker because the learning allows the attackers to evade detection and makes each new attack scenario easier to implement including taking less time. The evolution of generative AI, individuals, loosely federated groups, and opposition nation-states, can use the AI tool with little investment in training and education in coding to write malware, develop bots and launch more sophisticated attacks.

These attacks can be launched through a variety of means. These platforms for attack are often prompt injections, open-source code injection, data poisoning, and model evasion. Also, an attack can be initiated through using the administrative backdoor that many, if not all, developers leave in their software to allow easy updating, fix insertions, and problem identification. The use of the backdoor can allow the attacker to use the AI tool being used to become the attacker and download data to the attacker.

What do the attacks look like? As an example, an open-source, deep learning language model known as GPT-3 can learn the nuances of behavior and language. It could be used by cybercriminals to impersonate trusted users and make it nearly impossible to distinguish between genuine and fraudulent email and other communications. Phishing attacks could become far more contextual and believable. (https: pluralsight.com, The Impact of AI: Cybersecurity Challenges and Opportunities,newsletter, 10 November 2023)

One of the issues attending to this risk is that the attacker can infiltrate the network and reside without detection for long periods of time. The attacker can also evade detection by moving slowly and discreetly after identifying the targets within the system that they desire to attack, such as generating a computer "worm" that moves slowly but efficiently to identify and exploit valuable datasets.

What can be done by organizations to combat these attacks? Some organizations are investing in zero trust architecture (ZTA). ZTA is a data-centric security approach. It "assumes a breach, verifies identities, and grants the least-privileged access." Booz|Allen|Hamilton, Advancing Zero Trust Maturity Through Cyber Deception, Newsletter, March 2024. The system can reduce reaction time for attack identification

by providing clear signals of the intrusion. It also has the potential reduce cost for detection and handling, including isolation of the threat. The drawbacks to such a system is the initial investment, continual updating, and the need for highly skilled personnel. It also requires the endpoint, or the source or device being identified that is requesting access.

Several forms of attack have been discussed thus far, but perhaps one of the most frustrating and potentially harmful forms of attacks is the threat from an unmanaged endpoint. An endpoint is the device or system location that has requested access to a system, set of data, or individual's device. The matter is made even more difficult since many organizations are using legacy systems such as workstations, servers, employee established servers, and embedded devices such as printers. Such attacks are often called vulnerability attacks. Again, investment and time to identify legacy systems and hardware is a difficult roadblock to countering cyberattacks. Many legacy systems and hardware are invisible to those personnel with the responsibility to manage the organization's cybersecurity.

The one tool available to the organization is establishing decoy systems or hardware to ensnare the attackers. However, this approach is becoming less available due to the use of AI as a tool for attack or using the organization's system to conduct the attack, as it learns to identify such decoys.

Throughout this discussion the cost of cyberattacks and employing cybersecurity have been discussed. According to IBM®, the average cost of an attack to an organization was $4.45 million in 2023, which has set a new threshold. This cost is on top of the cybersecurity tools and systems that an organization has invested to combat these attacks. The study also noted that 42% of organizations surveyed have developed cyber fatigue and apathy. (IBM, Research Insights, https: IBM.com, 2024) These organizations have determined that nothing can completely prevent cyberattacks. The organizations are building the cost of such attacks into their products and services. The other costs being built into those products and services are the costs involving legal challenges due to attacks and release of information, including client proprietary and personal information.

The loss of proprietary and personal information is normally an incursion by ransomware into the system. While over 90% of malware attacks are a result of email use, the statistics are going up through the use of AI systems to identify the data desired. (Statista Research Services, Most Commonly Exploited Applications Worldwide from November 2021 to October 2022, statista.com)

Other costs driving the cost of cybersecurity are compliance costs, including regulatory mandates. These costs are expected to escalate in the coming years. *

Insiders that fail to update passwords or do not have multiple identification processes are escalating cost. These items can be handled through organizational governance

and the attending software procedures. However, many organizations through either cyber fatigue or awareness are not preventing the inside users from continuing to be a risk.

The recovery and identification of personal or proprietary information lost is also a cost because such organizations fail to have a recovery plan and operation in place. The time lost in identification of the source of the attack, not necessarily the attacker, and the time lost to recover are costs that are hidden until an actual event takes place. (Fines for Breaches of EU Privacy Law Spike Sevenfold to $1.2 billion US, as Big Tech Bears the Brunt, CNBC,18 January 2022, cnbc.com)

Open-source versus close-sourced generative AI

Definitionally open source is software development where all or part of the application's source code is released to the general public. It can be developed by a single voluntary source or by a decentralized voluntary group, which might be an organization or a loosely confederated group of individuals. Open-source code is generally open for use under a contract, copy left contract, which makes the code for updates and extensions open-source. Usually, the code is not copyrighted and available for all users. Some users have attempted to use open-source software as proprietary by modifying the code. This type of use also carries the same risk as open source that has not been converted to proprietary due to various weaknesses, backdoors, and other developmental issues that allow a cyberattacker to manipulate the code to gain access to the organization's systems and models.

Further issues with open-source exist in that most open-source software is not developed in an organized fashion wherein the group of developers could share issues, risks, and fixes. The other issue is that with open-source code the safety of use and risk identification and treatment are lagging due to the focus on development. Part of this problem set is the lack of responsible parties and difficulty in assigning responsibility following an attack.

Crowd-sourcing for identification of vulnerabilities is becoming more prevalent, but is not being done in any organized fashion, nor are alerts managed to make sure the user community is aware of the vulnerabilities. With generative AI, the role of communities of developers is even less defined currently and the focus is on function over security.

Some small users communities are developing risk analysis components, but the components are generally designed to specific, identified vulnerabilities. The cycle of development is lagging the threats.

Close-sourced is software development where the code is proprietary, not publicly available and can be created by an individual, group of individuals via a contract arrangement to maintain the proprietary use, or an organization solely under contract. Most of the closed-source software platforms available are developed by just a few AI laboratories. The focus is on the economic gain over the number of users and that monetization creates a greater demand for cybersecurity to be considered in the development, especially in generative AI platforms.
(*https://www.deloitte.com/uk/en/Industries/technology/blogs/open-vs-closed-source-generative-ai.html*)

Some of the closed-source software development firms have focused on generative AI platforms with agreements in place for cloud computing organizations to reduce various cybersecurity issues with cloud computing service organizations that make cybersecurity a priority. One caveat is that while it is a priority; it is not cybersecurity invulnerable. The cloud is a group of servers acting as a collective for storage of data, models, and other material. This material is generally proprietary and visibility into the cloud could afford the cyberattacker information as to market, designs, client proprietary information, personnel information, contract information, and other information of a sensitive nature.

Conclusion

Cybersecurity is and will continue to be a multitude of various risks. Many of the risks have costs that make resolving them in a continuous fashion too high for most small and medium-sized organizations currently. The risk of a cyberattack has been growing with the risk on one or more occurring in a year to any organization growing by 1000 plus percent during 2022. (Statista Research Services, Most Commonly Exploited Applications Worldwide from November 2021 to October 2022, statista.com)

When choosing to use an AI platform, one should study the risks, costs, and exposure in the public relations area. Many organizations have now resorted to asking clients to sign statements that they are aware the organization uses AI tools and that they have been briefed on the risks. Whether such statements will insulate any organization is still an open question as it has not been adjudicated.

Currently, both open- and closed source software development remain viable routes for individuals and organizations. The task is to be informed during the decision process.

Resources

https://aws.amazon.com/es/ai/generative-ai/security/?gclid=CjwKCAjw4_K0BhBsEiwAfVVZ_7pj62jT7EYlHnRmQJbE9TRw8H5O0JoudCmLE3Icf00_wyLvYWIBdRoC6A0QAvD_BwE&trk=d4e71091-28c9-48ac-ab5e-7c062ee9d2f0&sc_channel=ps&ef_id=CjwKCAjw4_K0BhBsEiwAfVVZ_7pj62jT7EYlHnRmQJbE9TRw8H5O0JoudCmLE3Icf00_wyLvYWIBdRoC6A0QAvD_BwE:G:s&s_kwcid=AL!4422!3!696756999061!p!!g!!secure%20artificial%20intelligence!20901657110!162153904058

https://centerforresponsible.ai/resources-pursuit-fairness-ai-product-development/

https://www.deloitte.com/uk/en/Industries/technology/blogs/open-vs-closed-source-generative-ai.html

https://economictimes.indiatimes.com/tech/technology/the-great-ai-debate-open-source-vs-proprietary-models-in-global-showdown/articleshow/107973022.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

https://www.engati.com/blog/ai-in-cybersecurity

https://www.esecurityplanet.com/cloud/cloud-storage-security-issues/

https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information

https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf

https://www.linkedin.com/pulse/what-some-examples-ai-powered-cyber-security-tools-david-knauer-larie/

https://www.precisely.com/blog/data-quality/data-validation-vs-data-verification

https://sloanreview.mit.edu/article/video-8-ai-security-issues-leaders-should-watch/

https://www.sophos.com/en-us/cybersecurity-explained/ai-in-cybersecurity

https://www.snowflake.com/guides/ai-cybersecurity/

https://www.technologyreview.com/2023/05/12/1072950/open-source-ai-google-openai-eleuther-meta/

https://www.telusinternational.com/glossary/data-validation

About the Authors

Ivano di Filippo

Rome, Italy

Applied Cognitive Neuroscience Scientist specializing in Project Management and AI
LinkedIn Profile | Official Website | Publications | Link to the book

Ivano di Filippo is a distinguished scientist in Applied Cognitive Neuroscience, focusing on project management and artificial intelligence. He currently leads the Cognitive Readiness Research Program, which is dedicated to advancing the mental preparation of leaders. From 2017 to 2019, Ivano served on the Board of Directors at the Italian Institute of Project Management (ISIPM), where he also holds certification as a Project Manager.

Educated in medicine at La Sapienza University of Rome, Ivano furthered his technical skills in computer science, working for ten years as a professional IT and Web programmer. His diverse expertise is enriched by over 30 years of studying and practicing Zen, integrating oriental disciplines into his professional and personal life.

In 2011, Ivano joined forces with Prof. Dr. Russell Archibald and Dr. Daniele Di Filippo in the international research program on Cognitive Readiness, eventually succeeding Dr. Archibald as the Program Director at his request.

In November 2022, he was appointed the Scientific Referent at ISIPM, continuing to impact the field with his innovative approach to integrating neuroscience into project management practices.

He is the co-author of the book “Cognitive Readiness in Project Teams - Reducing Project Complexity and Increasing Success in Project Management”. He can be contacted at

Dr. Josh Ramirez

Washington, USA

Dr. Josh Ramirez, PMP, NPPQ, is CEO of the Institute for Neuro & Behavioral Project Management, which he founded with Dr. Jodi Wilson. Josh is also co-author of the NeuralPlan (www.neural-plan.com) NPPQ master planner certification with Dr. Shari De Baets from Belgium, and he is an adjunct professor of project management, with experience that includes project management and project controls, including work at several national laboratories and other projects throughout the U.S. Department of Energy (DOE) complex. He has authored best practices for the DOE Energy Facilities Contractors Group and wrote for other project management periodicals. His doctoral dissertation is titled Toward a Theory of Behavioral Project Management. You can view an introduction to Josh and his colleagues' work in Behavioral Project Management at https://youtu.be/miqbagN_4dQ. The future of project management is designing PM methodologies around the beings that predict and deliver projects: humans. You can also listen to some of the podcasts Josh and his colleagues have been featured on, here: Behavioral PM: the Freakonomics Approach to Project Delivery with Dr. Josh Ramirez - https://pmhappyhour.com/ep077/; Neuroscience in Project Management - https://www.pmi.org/chapters/wdc/pmi-resources/pm-podcasts/pm-point-of-view-69; Tips from Behavioral Science - https://www.pmi.org/chapters/wdc/pmi-resources/pm-podcasts/pm-point-of-view-95.

Darrell Mesa

California, USA

Darrell Mesa, a Senior Program Planner / Scheduler and a dynamic intrapreneur, with extensive expertise in project management, including program planning, scheduling, and risk management. As a certified Project Management Professional (PMP), he has a demonstrated history of steering large-scale projects to success by applying industry best practices, with special proficiency in Earned Value Management (EVM), Critical

Path Schedule Management, and Work Breakdown Structure. His role as a Microsoft Project Practitioner at Denver Corporate Search showcases his ability to develop and update intricate MS Project schedules, adhering to stringent government regulations.

Darrell's professional journey is marked by significant roles that have allowed him to leverage his skills effectively. At Projitz LLC, as a Senior Program Planner / Scheduler, he enhanced project efficiency through meticulous application of Work Breakdown Structure and Critical Path Analysis. As a Senior Integrated Master Scheduler at Highbury Defense Group, he made notable improvements in program efficiencies through the execution of Integrated Master Schedules and the integration of Earned Schedule methodologies. A key achievement in his career was the development of 89 Project E-cademy training courses, which increased team productivity by 10%. In his capacity as a Learning Management Administrator, he demonstrated dedication to knowledge dissemination, using WordPress Tutor LMS to bolster team skills in Project Scheduling using Microsoft Project Professional and Project Web App.

In addition to his corporate roles, he is the founder of Influence IPM LLC, a business focused on Integrated Project Management, where he leverages his vast experience to provide cutting-edge project management solutions. More about his entrepreneurial venture can be found at influenceipm.com. Beyond traditional project management, he is also an active AI Influencer through his YouTube channel (Restless Minds), where he creates and shares content on AI advancements, fostering a community of tech enthusiasts and professionals keen on the latest in artificial intelligence. Based in Murrieta, California, he is keen on connecting with like-minded professionals and can be reached via email at darrell.mesa@pm-ss.org or through LinkedIn at https://linkedin.com/in/darrell-mesa-pmp-csm-4bbb8955.

Claudia Alcelay

Madrid, Spain

Claudia Alcelay, Product Manager, AI | PMP®, PMIACP, CSPO®, SAFe 5 is an experienced project manager specializing in AI with a deep background in innovation, particularly in driving the evolution of the EdTech sector. She has served for the European Commission and various ministries in Spain, Egypt, and France. She currently works as a Product Manager for AI with a focus on developing innovative solutions to enhance training portfolios. Additionally, her professional journey involves leveraging a

knowledge-based approach in data-centric AI models. She is an active community member, sharing her findings in her weekly newsletter, on LinkedIn, "My AI Reading List," and also serving as a panelist for MIT Technology Review and participating in the Advisory Council for Harvard Business Review (HBR). She can be contacted at caceley@gmail.com

Rebecca (Becky) Winston

Idaho, USA

Rebecca (Becky) Winston, Esq., JD, PMI Fellow, is a former Chair of the board of the Project Management Institute (PMI®). Becky has over 30 years of experience in program and project management, primarily on programs funded by the US government or their contractors.

Active in PMI since 1993, Rebecca Winston helped pioneer PMI's Specific Interest Groups (SIGs) in the nineties, including the Project Earth and Government SIGs, and was a founder and first co-chair of the Women in Project Management SIG. She served two terms on the PMI board of directors as director at large, Secretary Treasurer, Vice Chair (for two years), and Chair (2002). She was elected a PMI Fellow in 2005. She is also a member of the American Bar Association and the Association of Female Executives in the United States. She currently is the Executive Vice President of the College of Performance Management and the lead for their ISO standards committee given her 25 plus years of ISO experience.

She has served as an advisor to organizations such as the National Nuclear Security Administration (USA), U.S. Department of Energy (DOE) and the U.S. Department of Homeland Security (DHS) on topics ranging from Program and Project Management to project reviews, risk management, vulnerability assessments, software development and artificial intelligence. She served on the Air Force Studies Board for six years and serves the Intelligence Science Technology Engineering Group for the National Academies of Science, Engineering, and Medicine, as well as actively serving on many studies for the National Research Council. She can be contacted at rebeccawinston@yahoo.com